Capstone Synopsis- PGPCS-UTA June 2023

<Wenshan, Liu>

Name / Title of the Project:

Setting up Security Operations & Monitoring by using SIEM.

Objective / Problem Statement:

In this study, the Wazuh server was configured on a Linux workstation, whereas the target system was set up on a Windows PC. This approach facilitates the generation of security reports using a user interface.

Proposed Solution:

In the modern digital environment, safeguarding sensitive information and preserving the integrity of information technology systems are of critical significance, particularly for healthcare organizations that store confidential patient data. The main objective of this project is to provide a robust system of monitoring that can promptly identify, notify, and document potential security risks and threats promptly. In order to bolster the organization's cybersecurity stance, the objective of the project is to implement the Security Information and Event Management (SIEM) system Wazuh. This project entails the establishment and configuration of a Wazuh server to receive logs, the deployment of Wazuh agents on target systems, the construction of a security dashboard for event summaries, the generation of automated security reports, and the comprehensive analysis of these reports. By implementing this configuration, the business can effectively maintain the security of its development environment, thereby safeguarding the company's intellectual property and the sensitive data of its users.

Literature Review:

With the advent of data age, enterprises are increasingly facing the escalating threat of cyber-attacks. Many companies invest a larger portion of their IT budget towards addressing data breaches, resulting in reduced financial losses and reputational damage for the organization (Sim et al., 2023). Furthermore, cyber-attacks pose possible threats that are directly related to national safety issues. Under these circumstances, SIEM is employed to detect the attacks. (Patel, 2012). The Security Information and Event Management (SIEM) solution is designed to assist enterprises in identifying potential security threats and vulnerabilities, detecting anomalies in user behavior, and facilitating incident response (Mohd Ariffin et al., 2022).

Sim et al. (2023) asserts in their article that the Wazuh SIEM system offers number of significant capabilities. One example of a crucial function is the examination of log data. The Wazuh agent is responsible for gathering logs from the operating system and programs, which are subsequently uploaded to the Wazuh server. Wazuh will gather and analyze the system logs and any harmful actions. Furthermore, incident response enables administrators to enact designated response roles in the event that the target system encounters a potential threat. The Wazuh also enables administrators to remotely operate promptly in order to identify risks. Furthermore, Wazuh agents have the capability to remotely scan the target machine using anomaly detection. Setting up a scanning routine is beneficial for the detection of harmful viruses or suspicious activities. Lastly, the Visualization feature in Wazuh highlights the utilization of a customizable dashboard through a web user-interface. The Wazuh platform could be effectively managed and monitored. Users have the ability to generate specific reports using this user-friendly platform. In summary, Wazuh offers a wide range of practical tools for achieving a comprehensive system to monitor target machines, ensure cyber security, and mitigate potential hazards.

The concept of employing Security Information and Event Management (SIEM) systems for network protection in the context of a dam example is introduced by Luigi Coppolino et al. (2011). In this particular instance, the authors put out a proposal for an Open-Source Security Information Management (OSSIM) SIEM system developed by AlienVault. The purpose of this system is to oversee and analyze the events that are created by the security sensors of the dam. Furthermore, Coppolo et al. (2021) highlights the escalating vulnerabilities associated with cyber-attacks in the healthcare sector, namely inside smart hospitals, which are heavily dependent on interconnected information and communication technology (ICT) environments and Internet of Things (IoT) technologies. Their proposal aimed to enhance security and resilience against cyber threats by implementing a SIEM solution that improves data processing and event correlation capabilities. These two examples illustrate that the SIEM is capable of promptly detecting threats, ensuring a response time that meets the business process requirements with a significant level of safety.

Conclusion:

This study explains the utilization of SIEM for the purpose of identifying suspicious applications and monitoring malicious network connections. It has a chance to be utilized in various areas, including the health care industry. It offers an effective method to prevent data breaches or significant cyber-crimes in the real world. This project demonstrates the process of deploying the Wazuh system on the designated machine and monitoring the server. Furthermore, it illustrates the process of conducting an experiment to identify the failure of a login attempt in order to operate the system and uncover any potential dangerous applications. Lastly, the process of integrating data from logs and generating a report can be learned through the utilization of the visualization function.

Reference:

Coppolino, L., Sgaglione, L., D’Antonio, S., Magliulo, M., Romano, L., & Pacelli, R. (2021). Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes. SN Computer Science, 3(1). https://doi.org/10.1007/s42979-021-00858-4.

Luigi Coppolino, Salvatore D’Antonio, Valerio Formicola, & Romano, L. (2011). Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study

Mohd Ariffin, M. A., Darus, M. Y., Haron, H., Kurniawan, A., Muliono, Y., & Pardomuan, C. R. (2022). Deployment of Honeypot and SIEM Tools for Cyber Security Education Model In UITM. International Journal of Emerging Technologies in Learning (iJET), 17(20), 149-172. https://doi.org/10.3991/ijet.v17i20.32901

Patel, M. V. (2012). A practical solution to improve cyber security on a global scale.

Sim, D., Guo, H., & Zhou, L. (2023). A SIEM and Multiple Analysis Software Integrated Malware Detection Approach 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI),